FACULTEIT INGENIEURSWETENSCHAPPEN
DEPARTEMENT ELEKTROTECHNIEK – ESAT – COSIC
KASTEELPARK ARENBERG 10, BUS 2452
B-3001 HEVERLEE

KU LEUVEN

Crypto-biometric systems in the ePassport life cycle

CoSIC Internal Report

PhD Student: Christina-Angeliki Toli

Promotor: Professor Bart Preneel

Leuven, September 2013

1. Definition of the problem

With the globalization of our society we are increasingly engaged in transactions, both online and offline, with people we do not know. This has created a need for technologies based on reliability that allow individual identification and authentication in a way that cannot easily be abused. Physical or behavioral properties inherent to an individual are commonly referred to as biometrics [4]. Biometric systems have found their way to a wide range of application domains such as forensics, immigration and border control, or physical and logical access control [10]. Passwords compared to biometrics is that the second field is considered to be more secure and reliable but have an increased awareness of the privacy issues that come with their use. This discrepancy between security demands and privacy awareness has given rise to the field of biometric template protection [25]. Hide biometric data, prevent linking of hidden data and maintain the ability to authenticate or identify a person is some of the objectives of this project. The application will be focused on an improved version of travel documents embedding electronic chips called electronic passports (ePassports) [8].

Since August 2006 the Member States of the European Union have been required to issue electronic passports that contain a digital facial image, and since June 2009 they have been obliged to issue second generation of documents that also include two fingerprints [12]. The purpose of mandating issuance of ePassports has been to strengthen the link between the passport and the carrier of it, as well as to make it easier to verify the authenticity of the passport. With the increase in the numbers of ePassports in circulation the need arises to assess the security impact of the new technology. The Automated Border Control (ABC) systems are already in operation in several airports and the added functionality of these passports is being put to use for travel facilitation of European citizens [26].

The estimation of the relevant state-of-art possesses an important role at the phases of the research. Starting point seems to be the fingerprint recognition, with widespread use in passports, given the fact that fingerprints constitute the most famous biometric characteristics. One step further, our research will also rely on template protection schemes for Iris code representation [25,31,32,37]. Emphasis will be also given to crypto-biometrics in multiple modalities suitable for identity verification, trying to improve the available mechanisms and implemented the solutions for large scale deployment in order to meet the requirements for such an important performance as the electronic passports [10,21].

2. Strategic objective

The main objective of researcher's work is to demonstrate privacy enhanced solutions for the open problems related to ePassport life cycle. Specifically, the main goals are:

- Analyze crypto-biometrics in multiple modalities. Where we will indicate why biometric template protection is not a trivial task. Define the desired properties of a good template protection method relevant to fingerprint management and the requirements for electronic passport issuance.
- Strengthen privacy, designing protocols. In this way we will achieve the existence of private information queries based on crypto-biometrics.
- Assess the protection properties. The researcher will use a package of specific attacks for the proposed methods.
- Analyze the results and learn why they are effective. Generalize and provide frameworks to support the evaluation of the methods.

The approached solutions under this Ph.D. research will be used as a useful contribution to scientific projects such as those with main field the biometric identities investigating identity check for traveler privacy [4,12,18]. These works focus on providing trustworthy solutions for travel documents issuing processes, proposing algorithms and protocols for passports and suggesting technically-viable proposals that are acceptable within the ethical and legal contexts of the larger European Union. In this way, this project can improve ePassport security and usability, investigating processes and dealing with biometrics and their management in data bases. During this doctoral research should also be estimated the solutions from the view of the explorations into the operational, social, policy, and legal regulatory issues relating to identity, security, and privacy [8,13,26].

3. Description

In this chapter we will describe the planned activities and the basic motivation of their execution. Also, at the chapters below, we will analyze the methodology [4,18,22,23,28,29,32] in which these experiments and activities will lead to the goals that should be realized for a secure development of technical solutions and recommendations to overcome problems in the life cycle of an electronic passport.

The science of establishing the identity of an individual considering the physical, chemical or behavioral attributes of the person is defined as *biometrics*. These attributes or physical characteristics that we use to recognize individuals are referred to as modalities. The properties that are typically required from a modality, in order to be useful in an application such as the implementation of it in electronic passports, are universality, uniqueness, permanence, measurability, performance, spoofability and acceptability.[8,10,13,26] The *figure 1* shows an example of the modalities and their data representations that will be useful for this work.

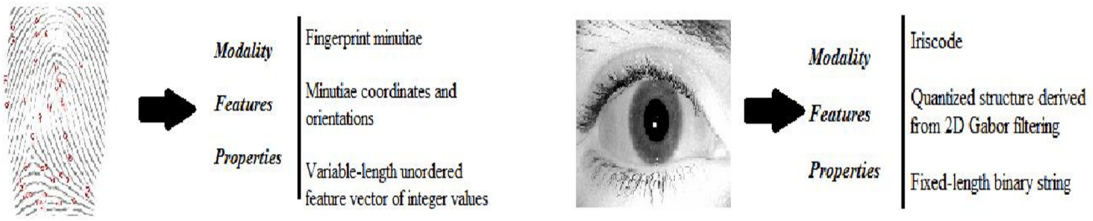

Figure 1: Fingerprint and Iris Code Representations

3.1 Biometric identity for safe travel document issuance

Because of higher technical security of ePassports, the importance of secure issuance procedures is increasing in the combat against identity fraud. The issuance of electronic passports is performed under coordination and control of a national government. Although travel documents can be issued to non-nationals of a country, the ePassport is usually only issued to country nationals. Although the technical specification of the ePassport is harmonized for the EU Member States, the issuance procedure and entitlement criteria for an electronic passport is regulated at a national level only and not in the remit of European Council decision, regulating the technical security of passports within Europe [12,19,22].

An ePassport for a false identity is a valuable tool for fraudsters [13]. Therefore, there are constant attacks on the issuance process. In order to estimate the importance of a safe travel document issuance, we should consider the threat scenarios which are listed below:

- Applying for an electronic passport under a false identity with genuine evidence, improperly obtained from another individual.
- Applying for a passport under a false identity, using manufactured evidence.
- Using a falsely declared lost or stolen electronic passport of someone who resembles the bearer.
- Apply for an ePassport with the intention of selling it to someone who resembles the bearer.
- Rely on staff to issue an electronic passport outside the regular procedure.

Using biometric systems, gaining knowledge from the existing systems and implemented cryptography in order to create a new generation electronic passport seems to be a promising technology [2,11,25,31]. In this way, using biometric data for purposes of authentication and identification requires agreement on rules regarding, what biometric data sets count as acceptable means of identification and how these data sets shall be collected, and under which circumstances travel documents that contain or reference these data sets shall be issued.

These agreements and rules belong to the types of conventions that will be mentioned at the end of the third chapter. They are conventions about when a person counts as self-identical in the eyes of legal authorities [20]. Both kinds of rules present particular challenges. In the first case, the challenge is to find data sets which are convenient to use for everyday purposes and yet difficult to steal and copy [2]. This challenge is, mostly of a technical nature. In the second case, the challenge is of a different kind. In the literature on biometric passports, this challenge has become known as the problem of "breeder documents" (cf. European Commission 2005: 42-43). [8] Breeder documents are the documents which are required to apply for a biometric passport, e.g., birth certificates. No matter how far we can increase the safety and reliability of the process of reading the biometric data from a passport, the passport itself will only be as safe and reliable as the bureaucratic process through which it was issued [12].

Implementing international standards for biometric travel documents, standards which are currently being discussed and developed, requires agreement on the issuance conditions of such documents [13]. From the perspective of states whose legal requirements for the issuance of passport and other international travel documents are relatively demanding, universally enforced, and based on reliable breeder documents, a call for high international standards in breeder documents will seem like a reasonable demand for border security. Also, considering the problem of breeder documents from the perspective of a citizen of a state that does not have a trustworthy bureaucracy in this regard. If state does not keep proper records of its citizens, or if its passport does no fulfill the latest technical requirements imposed by the most advanced states, or if its passport issuance process is not transparent enough, this citizen will effectively be excluded from international travel to a number of states and international travel will generally be very difficult.

Beyond the current issues of privacy and security of the citizens, EU, the U.S. and few other states agree on using biometric data and highly reliable breeder documents as the precondition for largely unrestricted freedom of movement between themselves, recognizing the meaningful sense of the words biometric identification or authentication practices [36].

3.2 Biometric template protection

Regarding the fact that ePassports contain biometric data that must be captured and then recognized and matched then we can talk about the main objective of biometric template protection, which is to protect a piece of iris code or fingerprint data that has to be used as a reference for comparison with another very similar but always different piece of data [23,28,29,31].

During this task, the confidentiality of the data should be protected in order to prevent impersonation and leakage of sensitive information. (Irreversibility property) This works in the same way as we are able to use a password when we can read it, we can use a biometric template to construct a new artificial sample that might pass a verification test. Secondly, during the process, it should be possible to compare unprotected data with protected data.

It is well known that, in case we want to protect a biometric template we cannot apply traditional data protection techniques for passwords applying a one-way function *f,* which is a cryptographic hash function or iterated variant, to a password *p* that is stored in a system during enrollment [31]. Finally, it should be possible to generate multiple protected references from the same characteristic. Usually called as the diversification property of template protection. Recall that biometric data are considered to be unique and in order to be used as identifiers for profiling, two protected references should not be comparable. This is often called unlinkability or indistinguishability property of protected templates.

In the literature [4,9,14,16,29,34,37], the template protection schemes divided into two main categories, reflecting the relevant process and again, separated to those that are based on feature transformation and the others are biometric cryptosystems. During the specific Ph.D. project for biometrics implemented in passports, the researcher will focus on techniques for error correction in order to cover the requirements for the design or the estimation of a good template protection scheme. As the *figure 2* below shows, the error correction techniques are used as a substitute for the comparison algorithm where two templates are considered to match based on the result of the decoding algorithm. The feature transform techniques are further divided into salting methods and non-invertible transformations. The difference between the two is that salting applies a transformation that is non-invertible under the condition that some parameters or a key are kept secret, whereas the other category is a one-way function that is also parameterized or key-dependent, but is considered to be hard to invert.

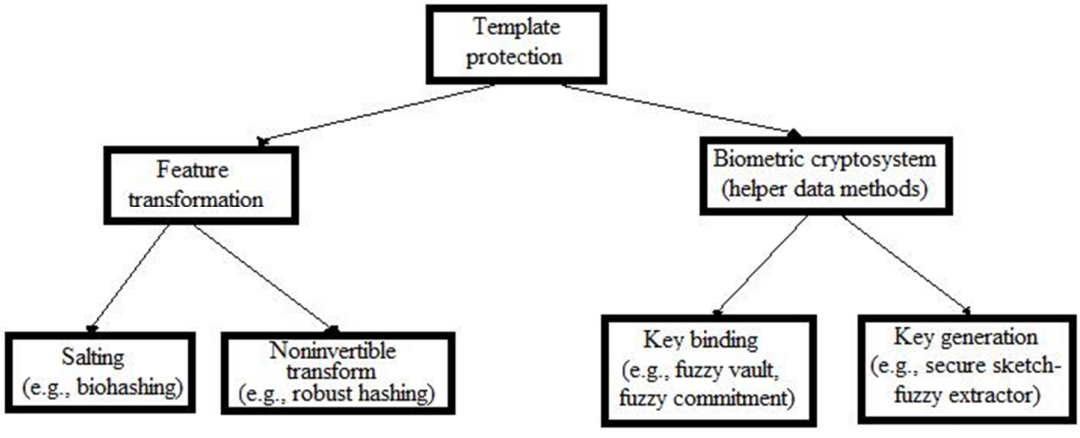

Figure 2: Categorization of template protection schemes

The techniques based on feature transformation are generally referred to as algorithms for cancelable biometrics. Other names of techniques as synonyms for biometric template protection are biometric encryption, untraceable biometrics, secure sketch, fuzzy extractor, helper data scheme, pseudo-identities, fuzzy commitment, fuzzy vault, shielding functions and random projection. The names of the biometric cryptosystem algorithms reflect the original purpose for which these algorithms have been designed. Their primary goal is to enable encryption using biometric data directly as a key or the extraction of a secret key that could be used in other cryptographic algorithms. These techniques, also, protect sensitive data and allow verification by verifying that the key extracted from a new sample matches the key that was registered during enrollment [31].

3.3 Crypto-biometrics in multiple modalities

During the project, the doctoral researcher will design crypto-biometrics techniques to the specific case of multiple modalities, suitable for identity verification and investigate the adaptation of these techniques for electronic passports and other applications. The research will be focused on the generation of a key from multiple modalities using the combination of fusing minutiae with iris feature and it will be based on cryptographic techniques [1].

Multi-biometric systems have improved the accuracy and reliability of biometric systems and one step further, the issue of recognition is operated on large scale datasets. For this reason, it is thought to be the missing key for the improvement of the new generation of ePassports. Combining technologies such as fusion, template protection for biometrics, we can provide a provable security and privacy and attain better rates for the process of recognition, that until nowadays remain elusive [4,18].

When we are taking about crypto-biometrics in multiple modalities, the issue of generating and sharing biometrics based on secure cryptographic keys should be addressed. In particular, the current literature proposes protocols which integrate multi-biometrics, in which information from different sources is combined [8,20,29]. These protocols allow generation and sharing of multi-biometrics based crypto-biometric session keys. Specifically, the mutual authentication matter approached with a lack of an extra involvement. The templates are revocable and thus protect user privacy [32]. The most distinctive feature of such a protocol is that it can integrate multi-biometrics and depending on the required security level, the choice of the biometric modalities to use can be made at runtime. This idea seems to be extremely important for the electronic passports, considering their process of use and the allegation of many different services between the countries [13,26].

One of the most important open problems for the research in the area of multi-biometric template protection is the production of a system like the *figure 3* where there is the capability of the incorporation of many different biometric templates.

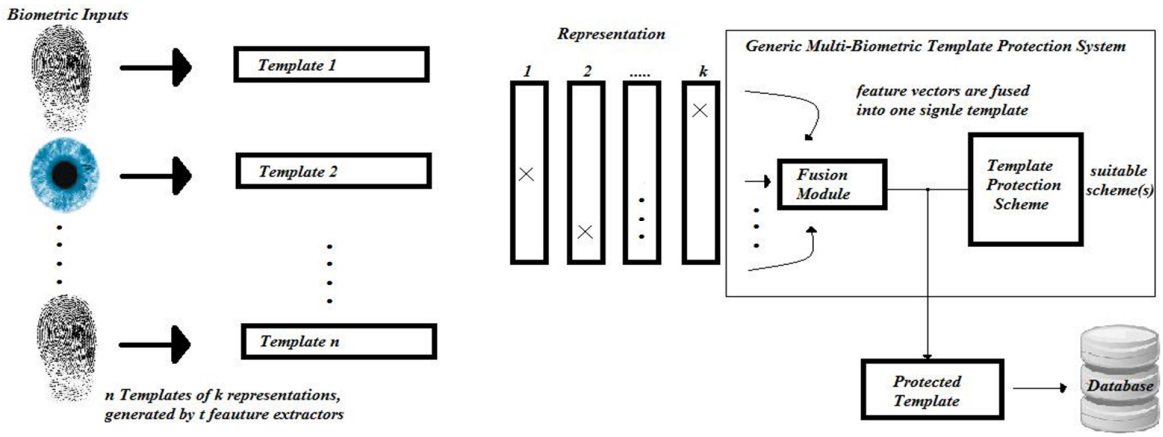

Figure 3: Proposed multi-biometric template protection system

Other challenges for future doctoral work constitutes the template alignment, the combination of modalities, the feature representation and the security, privacy issues of the system. During the third year of this doctoral research should be addressed the possible solutions, in order to evaluate the scalability of biometric schemes and estimated the security of any multi-biometric scheme with attention to irreversibility and unlinkability issues [1,17,19,31,32,33,37].

4. Usability, convenience, rights and obligations

In order to consummate the research must assure trustworthy results, including obligations and responsibilities, while enhancing the privacy of personal data. The final stage of this PhD project includes the study of the explorations into the operational, social, policy, legal regulatory issues relating to identity, security, and privacy that must be addressed by the solutions for the use of biometric data and agree with the current proposals for reform of privacy and data protection, published by the EU Commission on January of 2012. The researcher must understand some concepts and the importance of determining the main principles of data protection. This is a necessary condition in order to enhance trust in the use and processing of personal biometric data, for research security purposes [8].

As the passport constitutes a proof of identity, many frauds began to emerge. Consequently, an effort has been made all over the years to counter forgeries and counterfeits, which has allowed creating the ePassport, a secure passport containing biometric information. However, the current system is not perfect and some security issues have been found. The whole process can also be very long, especially on identity checkpoints where the speed is the main concern, as the people flow is really important, heterogenic and complex, which does not help to maintain a certain level of security and improve the usability of the ePassport [10].

During the creation process of the ePassport we should safeguard the integrity of biometric data in the chips. Many secure processes have been defined, and some of those involve the use of certificates.[16] Those certificates are specific to each country and every control check point needs to get those certificates in order to manipulate all the generated ePassports.[26] These kinds of constraints increase the complexity and create a gap in the security. Finally, the passport is used in different environments such as airports, frontier or maritime zone, and those areas do not have the same usability constraints. To sum up, we should also mention that the passport holder is not used to the manipulation of this document and consequently, some constraints are related to him.

Furthermore, the most important requirements for usability and convenience which must be noticed during this forth-year project are listed in categories such as functional related to usability, biometric related to usability, security, speed, standard compliance requirements, stability, hardware, data mining performance and more, but their analysis in depth is not a field that concerns the KUL researcher of the relevant project.

The analysis of requirements gives some recommendations and proposes some solutions to achieve those terms. Data mining mechanisms are useful for increasing the security and speed of the identity check process. Also, the identity check terminal is a complex integrated system composed of several hardware and software components that can be used in many different configurations, many usability requirements are necessary to have a usable system. Moreover it involves different kinds of users with slightly different priorities. For each specific use case, a subset of requirements can be defined but there are always common main requirements for first the speed of the check process and then the guidance process, the low error rate and the low false reject rate [33,34,36].

The determination of the applicable national data protection law is the starting point for every assessment, including a legal review, of data processing activities in which personal data, including biometric data, are used. The deal has to do with personal data, controllers, processors of the data on behalf of the controller and the processing. Data processing principles include the legitimate processing which requires a legal basis, the purpose specification and finality principles, the relevancy, adequacy and proportionality principles, the prior checking relevant to situations, the security and confidentiality, the prohibition of automated decisions and the rights to receive, access, correct or object information and finally the transborder data flows. Finally, the notification obligation should also be reviewed and additional privacy obligations should be imposed, as a matter of importance in research activities for electronic passports and the implementation of crypto-biometric systems on them.

5. Applicabilities

The results of this Ph.D. project could be used as a significant contribution to the FIDELITY initiative with an overall objective to demonstrate solutions for fast and secure real-time authentication of individuals at border crossings [8]. Crypto-biometric systems in the electronic passport life cycle will provide a more solid and attractive scientific basis for the improvement of the current systems. An important issue that concerns ministries and industrial markets from around the world. The doctoral researcher of the KU Leuven, consequently, will have the ability to promote the results of this work on an international level. Such a significant cause that will bring together a wealth of experience and knowledge in matters of security, identification documentation and issuance, as well as the technology linked to it.

As the demands for implemented digital identity technologies are increased, the project comes to provide a new proposal for the operation and the use of the future electronic passports standards, satisfying the privacy requirements of many government sectors and companies dealing with biometric security and privacy products.

Specifically, beyond the relevant educational institutions such as Katholieke Universiteit Leuven, Universities in Italy, Germany, Sweden, this technology has tremendous advantages in the social and legal fields of human life and the interest of all the partners that are involved in this project such as Bundeskriminalamt (BKA) which is the central agency for Federal Republic of Germany, Ministry of Security and Justice Netherlands, Ministère de l'Intérieur (France), Italian Ministry of Interior, Swedish Ministry of Defence and International Civil Aviation Organization (ICAO), shows the importance of this technology that covers diverse factors of identity management but also various economical, safety, security, efficiency and regularity issues.

Furthermore, Thales Computer and Network Security that has recently become the French market leader in civil biometric systems signing a new contract with France's national agency. Thales is one of Europe's leading players in the security market producing secure identity documents and operational control systems in over 25 countries. The company's experience in key technologies like sensors, networks and secure information systems, positions it as a world-class integrator of complex systems and value-added services. Techspace Aero and Belgacom Communications are also interested in the development of electronic passports. Other companies are Fraunhofer and Bundesdruckerei (Germany), Biometrika in Italy, Selex ES in United Kingdom and more as parts of Safran Aerospace-Defence Security an international company which is the world leader in multibiometric identification technologies and a major player in explosive detection systems and smart cards, developing products and systems. Company's businesses include criminal identification, border control, secure biometric access, payments, digital identity management, telecommunications, travel documents, defense and high-value infrastructures, circulation of goods and people, public events and emergency services.

References

[1] C. Roberts, “Biometric attack vectors and defences”, Computers and Security, vol. 26, no. 1, pp. 14–25, 2007.

[2] Bruce Schneier. Architecture of privacy. IEEE Security and Privacy, 2009.

[3] H. Gilbert, M. J. Robshaw, and Y. Seurin. HB#: Increasing the Security and Efficiency of HB+. In N. P. Smart, editor, EUROCRYPT, volume 4965 of LNCS, pages 361–378. Springer, 2008.

[4] A. Ross, K. Nandakumar, and A. K. Jain, Handbook of Multibiometrics, Springer, Berlin, Germany, 2006.

[5] N. Ratha, S. Chikkerur, J. Connell and R.M.Bolle IEEE Trans. Pattern Anal. Mach.Intell. “Generating cancelable fingerprinttemplates” ,vol. 29, no. 4, pp.561 - 572, 2007.

[6] O.Billet, J.Etrog, and H.Gilbert. Lightweight Privacy Preserving Authentication for RFID Using a Stream Cipher. In S. Hong and T. Iwata, editors, International Workshop-FSE,volume 6147 of LNCS, pages 55–74. Springer, 2010.

[7] Frank Breitinger and Harald Baier. Performance Issues about Context-Triggered Piecewise Hashing. In 3rd ICST Conference on Digital Forensics & Cyber Crime (ICDF2C) , volume 3, October 2011.

[8] EU-FP7 project. Trusted Revocable Biometric Identities.

[9] T.van Deursen and S. Radomirovic. Insider Attacks and Privacy of RFID Protocols. In S. Petkova-Nikova, A. Pashalidis, and G. Pernul, editors,EUROPKI, volume 7163 of LNCS, Springer, 2011.

[10] Dennis Kügler. Security mechanisms of the biometrically enhanced (eu) passport. Presentation at the Security in Pervasive Computing conference, Boppard, Germany, April 2005.

[11] Juels, A., Wattenberg, M. A fuzzy Commitment Scheme. In Proceedings of the 6th ACM Conference on Computer and Communications Security, Singapore, 1–4 November 1999.

[12] Technical Guideline TR-03110, Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Version 1.11, Bundesamt für Sicherheit in der Informationstechnik, 21 Feb 2008.

[13] Doc 9303 Machine readable travel documents Part 1 2. Technical report, ICAO, 2006. Sixth edition.

[14] Biometric System Laboratory - University of Bologna, “FVC2006: the 4th international fingerprint verification competition,” 2006.

[15] S. T. V. Parthasaradhi, R. Derakhshani, L. A. Hornak, and S. A. C. Schuckers, "Time-series detection of perspiration as a liveness test in fingerprint devices," IEEE Transactions on Systems, Man and Cybernetics Part C, vol. 35, no. 3, pp. 335–343, 2005.

[16] Koen Simoens, Julien Bringer, Hervé Chabanne, Stefaan Seys: A Framework for Analysing Template Security and Privacy in Biometric Authentication Systems. IEEE Transactions on Information Forensics and Security 7(2): 833-841, 2012.

[17] Vassil Roussev. An evaluation of forensic similarity hashes. Digital Forensic Research Workshop, 8:34–41, 2011.

[18] Bian Yang, Lisa Rajbhandari, Christoph Busch, Xuebing Zhou, Privacy Implications of Identity References in Biometrics Databases, 2012 Eighth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP). 18-20 July 2012. IEEE. pp. 25-30.

[19] Simoens, K., Tuyls, P., Preneel, B. Privacy Weaknesses in Biometric Sketches. In Proceedings of the 30th IEEE Symposium on Security and Privacy, Oakland, CA, USA, 17–20 May 2009.

[20] Patricia A. Norberg, Daniel R. Horne, and David A. Horne, The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors, Journal of Consumer Affairs, Vol. 41, No. 1, pp. 100-126, 2007.

[21] Karel Wouters, Koens Simoens, D. Lathouwers, Bart Preneel. Secure and Privacy-Friendly Logging for eGovernment Services. 3rd International Conference on Availability, Reliability and Security (ARES 2008), IEEE, 2008.

[22] Simone Fischer-Hübner, John Sören Pettersson, Mike Bergmann, Marit Hansen, Siani Pearson,Marco Casassa Mont, HCI Designs for Privacy enhancing Identity Management,"Digital Privacy: Theory, Technologies and Practices", Book Editors: Alessandro Acquisti, Sabrina De Capitani di Vimercati, Stefanos Gritzalis and Costas Lambrinoudakis, Auerbach Publications (Taylor and Francis Group), 2008.

[23] J. Bringer and V. Despiegel. Binary feature vector fingerprint representation from minutiae vicinities. In Proc. of the 4th IEEE Int. Conf. on Biometrics: Theory, applications and systems (BTAS'10), pages 1–6, 2010.

[24] J. Feng and J. Zhou "A performance evaluation of fingerprintminutia descriptors", Proc. Int. Conf. Hand-BasedBiometrics (ICHB), 2011.

[25] Yang, B.; Busch, C. Dynamic Random Projection for Biometric Template Protection. In Proceedings of IEEE 4th International Conference on Biometrics: Theory, Applications, and Systems, Washington, DC, USA, 27–29 September 2010.

[26] Jaap-Henk Hoepman, Engelbert Hubbers, Bart Jacobs, Martijn Oostdijk, and Ronny Wichers Schreur. Crossing borders: Security and privacy issues of the European ePassport. In Proc. IWSEC 2006: Advances in Information and Computer Security, number 4266 in LNCS, pages 152{167. Springer, 2006.

[27] Biometric System Laboratory - University of Bologna,“FVC2006:the 4th international fingerprint verification competition” 2006.

[28] A. Ross, J. Shah, and A. K. Jain, “From template to image: reconstructing fingerprints from minutiae points,” IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 29,no. 4, pp. 544–560, 2007.

[29] X. Boyen, “Reusable cryptographic fuzzy extractors,” in Proceedings of the ACM Conference on Computer and Communications Security (ACM CCS ’04), pp. 82–91, Washington, DC,USA, October 2004.

[30] L. Nanni, A. Lumini, M. Ferrara and R. Cappelli, "Learning for combining fingerprint matchers: a case study FVC-OnGoing", in Elizabeth T. Mueller, Neurocomputing: Learning, Architectures and Modeling, Nova Publishers, 2012.

[31] Christian Rathgeb and Christoph Busch. Multi-Biometric Template Protection: Issues and Challenges, New Trends and Developments in Biometrics, Dr. Jucheng Yang (Ed.), ISBN: 978-953-51-0859-7, 2012.

[32] R. Cappelli, M. Ferrara and D. Maltoni, "Minutia Cylinder-Code: a new representation and matching technique for fingerprint recognition", IEEE Transactions on Pattern Analysis Machine Intelligence, vol.32, no.12, pp.2128-2141, December 2010.

[33] M. Ågren, M. Hell, T. Johansson: On Hardware-Oriented Message Authentication IET Information Security, Vol. 6, No. 4, pp. 329-336, 2012.

[34] Przemysław Błaśkiewicz, Mirosław Kutyłowski “Security and Trust in Sensor Networks”. Monographs in Theoretical Computer Science, pp 697-739. An EATCS Series 2011.

[35] B. Shanthini, S. Swamynathan “A Secure Authentication System Using Multimodal Biometrics for High Security MANETs.” Advances in Computing and Information Technology. Communications in Computer and Information Science Volume 198, 2011.

[36] Mina Deng, Kim Wuyts, Riccardo Scandariato, Bart Preneel, Wouter Joosen: A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements. Requir. Eng. 16(1): 3-32, 2011.

[37] D. Maltoni and R. Cappelli, Advances in fingerprint modeling, Image and Vision Computing, vol.27, no.3, pp.258-268, February 2009.